

## CLAIMS

What is claimed as new and desired to be protected by Letters Patent of the United States is:

- 1           1.     In a gaming machine, a method of authenticating a media device comprising:  
2                 setting an address pointer ADDR to a first next memory location in said media  
3 device;  
4                 determining whether said next memory location is a last memory location to be  
5 authenticated in said media device;  
6                 applying a hashing algorithm to the contents of said next memory location and  
7 updating a key-value;  
8                 adding a predetermined number N to said ADDR such that the next ADDR =  
9 ADDR+N;  
10                setting the next ADDR to the next memory location in the media device to be  
11 authenticated;  
12                repeating the determining, applying, adding and setting steps until the next ADDR  
13 is equal to said last memory location;  
14                determining whether said key-value is equal to a predetermined key;  
15                passing authentication if said key-value is equal to said predetermined key,  
16                failing authentication if said key-value is not equal to said predetermined key.

1           2.     The gaming machine utilizing the method of claim 1, wherein said first next  
2     memory location is a first memory location of said media device.

1           3.     The gaming machine utilizing the method of claim 1, wherein said last memory  
2     location is not the last memory location of said media device.

1           4.     The gaming machine utilizing the method of claim 1, further comprising:  
2                 calculating a random number S, wherein S is an integer from 0 to N; and  
3                 adding S to N such that  $N=S+N$  prior to setting said address pointer ADDR to the  
4     first next memory location in said media device

1           5.     The gaming machine utilizing the method of claim 4, wherein said predetermined  
2     key is equal to Z(S), such that Z(S) is equal to one of S predetermined keys.

1           6.     The gaming machine utilizing the method of claim 5, wherein Z(S) is calculated  
2     and stored prior to a first time the gaming machine is authenticated.

1           7.     The gaming machine utilizing the method of claim 1, wherein the predetermined  
2     key is calculated and stored prior to a first time said gaming machine is authenticated.

1           8.     The gaming machine utilizing the method of claim 1, further comprising:  
2                 calculating said predetermined number N such that N is equal to a number from 1  
3     to P, wherein P is less than a number of memory locations in said media device to be  
4     authenticated; and  
5                 wherein said setting said address pointer ADDR to a first next memory location in  
6     said media device comprises setting ADDR to N.

1           9.     The gaming machine utilizing the method of claim 8, wherein said predetermined  
2     key is equal Z(P) such that Z(P) is equal to one of P predetermined keys

1           10.    The gaming machine utilizing the method of claim 9, wherein Z(P) is calculated  
2     prior to a first authentication of said gaming machine.

1           11.    The gaming machine utilizing the method of claim 1, wherein said hashing  
2     algorithm is a SHA-1 algorithm.

1           12.     The gaming machine utilizing the method of claim 1 further comprising resetting  
2     said address pointer ADDR to said first next memory location in said media device after passing  
3     authentication such that said method repeats continuously until said media devices fails  
4     authentication or said gaming device is turned off ;

1           13.    A gaming machine comprising:  
2                   a user interface; and  
3                   a central processing unit (CPU) coupled to said user interface, said CPU  
4 comprising:  
5                   a processor;  
6                   a first media device coupled to said processor, said first media device  
7 adaptable to store data in a plurality of memory locations;  
8                   a second memory coupled to said processor, said second memory adapted  
9 to contain executable program code, said executable program code further comprises a plurality  
10 of instructions configured to cause said processor to determine the authenticity of said data in  
11 said plurality of memory locations, said instructions include instructions for:  
12                   performing a hash calculation on a sample of memory locations  
13 from said plurality of memory locations and calculating a key-value from said sample of memory  
14 locations; said sample of memory locations being a number of memory locations that is less than  
15 said plurality of memory locations;  
16                   comparing said key-value to a predetermined key;  
17                   authenticating said data stored in said plurality of memory  
18 locations if said key-value is equal to said predetermined key; and  
19                   not authenticating said data stored in said plurality of memory  
20 locations if said key-value is not equal to said predetermined key.

1           14.    The gaming machine of claim 13 wherein each one of the memory locations in  
2   said sample of memory locations are separated by N memory locations.

1           15.    The gaming machine of claim 14, wherein said instructions further include  
2   instructions for selecting the number N from a random number between zero and the number of  
3   memory locations in said plurality of memory locations.

1           16.    The gaming machine of claim 14, wherein the number of memory locations in  
2   said plurality of memory locations is equal to the total number of memory locations in said first  
3   media device.

1           17.    In a gaming machine that is turned on, a method of repeatedly authenticating a  
2   portion of a media device, said method comprising:

3                reading a plurality of memory locations in said media device wherein said  
4   plurality of memory locations are spaced from each other, said plurality of memory locations  
5   being less than a total number of memory locations in said media device;

6                after reading each memory location, calculating a hash value and using said hash  
7   value to update a key-value until all said plurality of memory locations are read and a final key-  
8   value is determined;

9                comparing said final key-value to a predetermined key;

10              passing said portion of said media device as authentic if said final key-value is  
11   equal to said predetermined key and repeating said reading, calculating and comparing steps

12              failing said predetermined portion of said media device as authentic if said final  
13   key-value is not equal to said predetermined key and halting operation of said gaming machine.

1           18.    The method of claim 17, wherein said portion of said media device is equal to all  
2   the memory locations in said media device.

1           19.    The method of claim 17, wherein said plurality of memory locations are equally  
2   spaced from each other.

1           20.    The method of claim 17, wherein said plurality of memory locations are equally  
2 spaced from each other by a number  $N$ , such that  $N$  is randomly selected each time the step of  
3 reading is performed,  $N$  is equal to a number that is less than the total number of memory  
4 locations in said media device

1           21.    The method of claim 20, wherein  $N$  is randomly selected from an number that is  
2 less than 20.

1           22.    The method of claim 17, wherein said plurality of memory locations are equally  
2 spaced from each other and the first memory location read is a random number  $S$  from a first  
3 possible memory location that can be read.

1           23.    The method of claim 22, wherein  $S$  is recalculated prior to said reading step.